Rüstungskontrolle im Cyberspace
Perspektiven der Friedenspolitik
im Zeitalter von Computerattacken

Internationale Konferenz
29./30. Juni 2001, Berlin

HEINRICH
BÖLL
STIFTUNG

Multilateral IT Security - A Question of Social Organisation and Culture

A Plea for a More Comprehensive Inquiry

by
Olaf Winkel*

For some time now there has been talk in the media that information warfare and cyber-terrorism pose an increasing threat to critical infrastructure. Meanwhile, calls to prevent an electronic arms race have become more frequent. This development has positive as well as negative aspects.

On the positive side, society and politics are becoming more sensitive toward the new problems which arise from an increasing transfer of social functions to electronic networks. On the negative side this approach to information technology (IT) security paints an insufficient picture of the breadth and multifaceted nature of the issue.

In several respects such a narrow outlook can lead to further problems. First of all, the perception of potential hacker attacks solely as attacks against military targets or as acts of terrorism can easily lead to a one-sided treatment of the problem, i.e. as a problem of internal and external security – an unreasonably limited view.

Secondly, the demand to protect critical infrastructure and the voices warning of a high tech arms race can lead to a perception of the matter as purely technical.

Thirdly, the call for a return to disarmament diplomacy is an inadequate response to the new threats of the electronic age. The belief that it is possible to contain new threats by making

I would like to thank Jan Öhlmann (scientific co-worker of the research project on IT innovation and IT security at Münster University, promoted by the MSWF NRW) for his help concerning the translation, the ideas he contributed, and the support he provided.

use of traditional structures and means is contradicted by the experience of the last few years.

In light of this, an alternative approach is proposed. This approach is characterised first of all by the examination of questions to do with IT security from an integrated perspective spanning multiple fields of politics; secondly by the fact that special attention is directed not toward traditional forms of containment, but toward the possible creation of new forms of security; and thirdly by the promotion of IT security as a creative process, with its central challenges situated less in technical areas and more in areas of social organisation and culture.

An integrated perspective on these new security problems is especially necessary in view of the experiences gained from the controversy concerning cryptography, particularly in the US. In this controversy, one side primarily classified cryptography as a weapon of war and assigned it to the military and secret services, while the other side saw in it a central component of an information society’s infrastructure. The move into an information society involves extensive decisions about the distribution of chances and risks. The divergent positions resulted in numerous irritations and conflicts – conflicts that have obstructed a more rational scrutiny of the problem for years.

An integrated approach to IT security does not obstruct investigations into individual areas -- be it, for instance, into central questions of internal and external security, protection of civic freedoms, or the organisation of IT security solutions at the level of international policy. Such investigations become all but superfluous – an integrated approach will only make them more meaningful and productive. The setting of priorities enables us to situate separate results and impressions within one framework thus making sense of findings in a number of different areas of research and thought.

Seen solely from the vantage point of arms control and disarmament, IT security has to be ineffectual. The attacks discussed here are characterised by the fact that they can be executed by an unknown number of aggressors, from areas far apart, and with quite variable motives. In addition, not only is it almost impossible to detect the preparation of such attacks, they can also be executed from a position of obscurity. Attacks that do not target the availability of information and communication but its confidentiality may result in damages that may remain unidentified over long periods of time, even permanently.

Under such conditions, conventional forms of conflict resolution and conflict prevention – which, as they were designed for Cold War conflicts, have already been proofed ineffectual in recent civil wars – appear hardly capable of delivering the desired effects. This of course still leaves the possibility to negotiate international treaties, for example, for the proscription of software anomalies or the renouncement of hacker attacks in the context of military and secret service operations. Such treaties would, however, have no binding effect whatsoever on the signatories because such regulations could never be effectively controlled. Thus, such treaties would be as effective as the statutory control of cryptography.

An extensive inspection of the controversy over the use of cryptography appears instructive here. This conflict forcefully shows how much traditional political and diplomatic structures, cultures, as well as traditional sociological perceptions and methodologies are outmanoeuvred by the new security considerations of a digital information society.

It is not new to view the promotion of IT security less as a technical and more as a problem of social organisation and culture. For some time this has already been the approach of many of those specialists who deal with IT security as administrators or advisors in businesses and bureaucracies. The transfer of this concept to superordinate levels – to society as a whole as well as to the international system – therefore appears to be only obvious.

The fact that organisational and cultural aspects play a decisive role in business and administrative circles can be attributed particularly to three reasons. Firstly, network security cannot be created once and for all but needs to be continually recreated. The variation of threats and technical innovations very much requires ongoing adaptations. Secondly, the trustworthiness of a technical system plays just as large a role as does its actual reliability. As a socio-technical system can be attacked and disabled in both its dimensions, it needs protection on either side. Factual security in one context can always be improved by technical, organisational, and personal security precautions in a relatively short time. The promotion of trust presupposes among other things an adequate social-institutional integration of the technical system – a difficult and lengthy task. The third reason for looking at the promotion of IT security as an organisational and cultural as well as an engineering challenge, arises from the fact that it represents not only a scarce, but also a relative resource, a resource which can denote different things for different players. Consequently there will arise conflicts of interest; handling them rationally will become a crucial requirement.

The paradigm of multilateral security could be a way to achieve this goal not only in individual areas of application, but also in societal and inter-societal contexts. Multilateral security is to consider the security interests of all parties involved in an act of communication or co-operation by way of compromises and compensations, and to distribute the remaining risks in a generally acceptable manner. Such an approach leads not only to a substantial increase in reliability, but also to an increase in trustworthiness and thus to the acceptance of new information technologies. Multilateral security can be put into practice in two ways – on the one hand by an appropriate technical systems organisation, and on the other hand, by the development of social structures and cultures which enable a rational, socially compatible, and result-oriented settlement of respective conflicts.

There are no ready-made solutions for an effective, acceptable, and sustainable handling of security problems. Rather the development of sustainable security solutions presupposes the consideration of the specific conditions in each individual case. Therefore, the promotion of IT security requires the inclusion of as many users as possible, else it will hardly have a chance to succeed.

To achieve this, it is important, though not sufficient, to distribute a technical security system which is efficient, economical, and easy to use. Furthermore a rational organisation of security processes, based on effective security management and rooted in a sustainable security culture, is needed.

Generally speaking the security process can be divided into five phases: First, problem perception and problem communication; second, handling of conflicts of interest by means of compromise and compensation; the next three phases facilitate the planning, execution, and control of technical and personal security precautions. By identifying new problems, which can be both the results of progress controls and of environmental monitoring, the security process is started anew (in terms of the cybernetic principle).

Security management can be described as the way in which security processes are devised institutionally and functionally. Security culture is a system of value conceptions -- ways of thinking -- and action patterns, embodied in the collective identity of a social unit, which guides its members in dealing with security threats, and which therefore is to be regarded equally as the base and the result of security management. Seen from this perspective it appears appropriate to subordinate the question, as to how an arms race in cyberspace can be prevented through arms control and disarmament, to the question as to how a globally devised IT security architecture can be developed between market, power, and society. Such a global IT security architecture would have to account for the organisational, cultural, and political aspects of IT security as well as for the technical aspects, and it would have to enable different groups to communicate and co-operate in the virtual world of the networks without having to accept unreasonable risks.

Isolated elements of such thinking can already be found in the stance that Washington is taking on the issue of the protection of critical infrastructures -- although the strategy of a public-private partnership is still generally endorsed in this area of policy. This new facet, however, cannot compensate for the fundamental deficiency of the US approach, which consists of Washington's seeking to apply a primarily nationally based solution to a global problem. Consequently, Washington is once again facing criticism for placing world leadership above the need for a collaborative partnership.